THE HIGH COURT
JUDICIAL REVIEW

Record No. 2013/765/JR

BETWEEN:

MAXIMILIAN SCHREMS

APPLICANT

AND

DATA PROTECTION COMMISSIONER

RESPONDENT

OUTLINE WRITTEN SUBMISSIONS

Filed on behalf of the applicant on the 8th day of April 2014 by Ahern Rudden Solicitors, of 5 Clare Street, Dublin 2.

Overview / Background

1. The Applicant is a law graduate from Austria and a customer of a social networking service known as "Facebook" operated by Facebook Ireland Ltd.
2. Users of Facebook must register before using the site after which they may create a "personal profile", add other users as "friends", exchange messages, upload pictures and use many other functions. Facebook has in excess of one billion users worldwide.
3. The Respondent is charged with the safeguarding of private data of individuals such as the Applicant in Ireland. Officials, similar in function to the Respondent exist in all other European states, and the safeguarding of private data is designed to be ensured under the provisions of EU Directive 95/46/EC. In Ireland the system in place designed to ensure compliance with data protection law is set out in the Data Protection Acts 1988-2003 (DPA).
4. It is a key element of EU Directive 95/46/EC and the DPA that data may not be transferred to a non-EEA country where an "adequate protection" level of data protection is not available.
5. The European Commission may find that a third country provides for such an "adequate protection". While this was not found for the United States in general, the European Commission has allowed for individual companies in the United Stated to "self-certify" under the so-called "Safe Harbour" rules. Such companies are then deemed to provide for an "adequate protection" under the conditions of Commission decision 2000/520/EC, known as the "Safe Harbour" decision.
6. The "Safe Harbour" system allows for the transfer of data to the United States, in this case by Facebook Ireland Limited to Facebook Inc, so long as the recipient in the USA has "self-certified" compliance with Safe Harbour and operates under the Safe Harbour rules.
7. The complaint and the subject matter of these proceedings relates to the transfer of data (which the Applicant says is unlawful) by Facebook Ireland Limited to its parent company in the United States of America, "Facebook Inc". All data (including the Applicant's personal data) is transferred by Facebook Ireland to Facebook Inc, for the purpose of "processing" that data in the United States.

8. Facebook Inc had "self-certified" under Safe Harbour, so, *prima facie*, the data export from Facebook Ireland Ltd to Facebook Inc is lawful.
9. However, simply put, the Applicant complained, that the transfer of data to Facebook Inc by Facebook Ireland Limited:

   a) breached different principled of the Data Protection Acts 1988-2003

   b) breached the conditions of Safe Harbour Decision

   and was thereby unlawful.
   Only if the Respondent would find that the Safe Harbour Decision would allow for such a transfer the Applicant additionally claimed, that in this case this executive decision of the European Commission would violate superior law, namely Directive 95/46/EC, Article 8 ECHR and Article 8 CFR.
10. The Respondent, on the basis that it was "frivolous and vexatious", refused to entertain or consider the Applicant's complaint and it is that refusal that is sought to be quashed in these proceedings.
11. These legal submissions include argument raised in the Complaint.

Reliefs Sought

The reliefs sought in these proceedings are as follows:

1. A Declaration that the failure or refusal of the Respondent to investigate a complaint filed by the Applicant with the Respondent on the 25th June 2013 in respect of Facebook Ireland Limited and "PRISM" (hereinafter referred as "the complaint") is unlawful.
2. An Order of mandamus compelling the Respondent to investigate the complaint and make a formal decision under Section 10(1)(b) Data Protection Act (DPA).
3. An order of certiorari quashing the decision of the Respondent expressed in the letter dated the 23rd July 2013, (hereinafter referred to as "the refusal decision") to refuse to investigate the complaint.
4. The costs of these proceedings.

Grounds

Ground 1

Ground 1 states:

"By relying to the extent that was done on the EU Commission Decision C2000/520/EC the Respondent unlawfully fettered his own discretion. It was irrational to rely upon this Decision in circumstances where the Applicant's complaint is specifically contesting its validity and arises from facts that were unknown or did not exist at the date of EU Commission Decision C2000/520/EC. EU Commission Decision C2000/520/EC can no longer represent good law in the light of those revelations and the passage of time and by reference to higher ranking law (Directive 95/46/EC, Article 8 ECHR and Article 8 CFR). In addition the Respondent did not consider the limitations of exceptions in the EU Commission Decision C2000/520/EC"

Fundamentally it will be argued that, in the light of the then recent revelations by a former contractor with the National Security Agency, Edward Snowden and of admissions by the USA authorities that the so-called “PRISM” program existed, it was clear that, despite the "self-certification" by Facebook Inc. under the Safe Harbour system an “adequate protection” was factually not provided.

Further it will be argued that there was in fact an ongoing and massive breach of the Safe Harbour certification by Facebook Inc., since its operations enabled direct access to all personal data of users by the National Security Agency (NSA). This permanent and bulk access was not strictly necessary for purposes that are excepted from Safe Harbour rules. Facebook Inc. breached the European Commission’s Safe Harbour Decision by cooperating with the NSA or by failing to prevent such access by the NSA.

It will be submitted that the Data Protection Commissioner, in refusing to investigate the Applicant's complaint, was operating under a "conclusive presumption" that, because Facebook Inc. had self-certified under Safe Harbour, that there was no basis to investigate the complaint and that it was "frivolous and vexatious". However Article 3 of the Safe Harbour decision (2000/52/EC) g allows the Data Protection Commissioner to suspend the transfer of data if there is a risk that the privacy of data subjects is violated, despite the fact that Facebook Inc. has “self-certified” under Safe Harbour. Furthermore the failure to even consider whether the permitted exceptions to the protections of the Safe Harbour Decision were applicable (which they were not) was also in breach of duty.

It was irrational for the Respondent (at least in the context of the validity / enforceability at the time of taking the impugned decision) and a "circular argument" to consider, for those purposes, that he was “bound” by exactly the decision that was contested by Applicant. This would turn an executive decision into an “absolute” law that could not be contested even if it were in violation of Directive 95/46/EC, Article 8 CFR and Article 8 ECHR.

The judgment of the CJEU in the joined cases of N.S. v United Kingdom and M.E. v Ireland (C-411-10 and C-493-10) will be referred to in support of the argument that such an approach is impermissible under European law. The Data Protection Commissioner was not entitled to "turn a blind eye" on such relevant factors (the then recent revealations made by Edward Snowdwen and the publicised reaction to same) going to the core of the protection of fundamental rights.

Ground 2

Ground 2 states:

"The opinion of the Respondent that the complaint was frivolous and vexatious was irrational in the light of the evidence put forward. In circumstances where it was brought to the attention of the Respondent that other Data Protection Commissioners in other EU states were treating similar and almost identical complaints very seriously and that the European Commission is reviewing its Decision C2000/520/EC it was irrational and unreasonable for the Respondent to

form such an opinion as expressed in the decision and to base a refusal to investigate thereon".

Fundamentally it will be argued that for a legal argument to be "frivolous or vexatious", as claimed by the Respondent in this case, such an argument must either be found to be false by a superior authority (e.g. clarification by the lawmaker, case law), found to be false or unfounded by other relevant authorities or in no way arguable given what was before a decision maker.
It will be submitted that in the instant situation the opposite is the case. : The superior authority that issued the relevant Safe Harbour decision (the European Commission) has voiced the same legal opinions and concerns as the Applicant (see appendix 1). Other relevant authorities (namely all European Data Protection Authorities that issues any opinion on the matter) have made the same legal findings as the Applicant, or have at least voiced the same legal concerns as the Applican (see appendix 2). Even the European Parliament, the superior lawmaker, has voted for abolishing the Safe Harbour system based on the same concerns as at the Applicant raised.

It will be submitted that the scheme of the Safe Harbour system expects that the law does not stop at self-certification of a US entity, but also anticipates that this US entity will follow these rules.

In addition it will be argued that the fact that an executive decision may not violate superior law and has to be interpreted in line with superior law (in this case Article 8 ECHR, Article 8 CFR and Directive 95/46/EC) is a fundamental principle of the European legal system and is as such in no way "frivolous or vexatious" (see e.g. CJEU in the joint cases C-465/00, C-138/01 and C-139/01).

Grounds 3 & 7
Ground 3 states:

"The refusal to investigate the Applicant's complaint was in breach of EU law, in particular the provisions of Directive 95/46/EC and Article 8 CFR. Article 25(1) of Directive 95/46/EC requires a member state to ensure that a transfer of data may only take place where the destination third country ensures an adequate level of protection.

In the light of the recent revelations concerning spying by the intelligence services of the United States of America and the making available on a large scale of private data to the said intelligence services it was irrational for the Respondent to conclude or be satisfied that, in the United States of America, an adequate level of protection was in place".

Ground 7 states:
"The Respondent failed to carry out any proper level of investigation as to whether the complaint was frivolous and vexatious and thereby failed in his duty to investigate".

It will be argued, that there is a duty on the member states and all its authorities, lawmakers and courts, to not only not intervene with the fundamental rights of a person, but also defend the fundamental rights of a person against third party violations. In this case the Respondent had a duty under Article 8 CFR (and Article 8 ECHR) to take all reasonable steps to protect the Applicant against an illegal use of his personal data.
The same is true for the duties of Ireland and the Respondent under Article 25(1) of Directive 95/46/EC, which prohibits a transfer of data to a country which does not provide for an adequate protection.
It will further be argued that the Respondent's view that the Safe Harbour decision from the year 2000 would have envisioned a form of bulk collection that was not even imaginable a year ago is irrational. The argument that the European Commission would have accepted such an unimaginable form of surveillance is missing any substance.

Ground 4
Ground 4 states:

"The Respondent erred in law in ascribing the meaning to the words "frivolous and vexatious" in the context of the Data Protection Acts as set out in the letter of the 11th October 2013. The Respondent acted unlawfully in ascribing a certain meaning to those words when the Respondent's published policy and case law ascribes a different meaning to them."

In relation to the question if the complaint was "frivolous or vexatious" the following will be submitted in relation to <u>all grounds that deal with this question:</u>

<u>Three Forms of Decisions</u>
It will be argued that there are three possible kinds of complaints under Section 10(1)(b) DPA:
a) complaints that are <u>justified</u> and upheld in a formal decision,
b) complaints that are <u>not justified</u> and rejected in a formal decision, and
c) complaints that are clearly less than just "not justified", but that are "<u>frivolous or vexatious</u>" so that they need not even be considered by the Commissioner;

It is submitted that the aim of the "frivolous or vexatious" exception can only be to dispose of complaints that are obviously absurd and only burdensome to the administration.

Deeming a complaint to be "frivolous or vexatious" can theoretically be misused by the Respondent to also dispose of complaints that might be controversial, complex and burdensome, but still justified. By finding that a complaint is "frivolous or vexatious" the Respondent can not only bypass his duty to make a decision under Section 10(1)(b) DPA, but the complainant also loses his right to an appeal to the Circuit Court. Most complainants will be unable or unwilling to go through a Judicial Review, just to restart the procedure before the Respondent. This very powerful exception must therefore be used and

interpreted with utmost caution in order to avoid misuse and a violation of EU law.

Definition of "frivolous or vexatious"

> The Respondent has stated that the complaint is "frivolous or vexatious". The question arises what should be considered "frivolous or vexatious". In Nowak v. The Data Protection Commissioner ([2012] IEHC 449) the High Court stated: *"20. (…) That section refers to complaints that are frivolous or vexatious. However, I do not understand these terms to be necessarily pejorative. Frivolous, in this context does not mean only foolish or silly, but rather a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome, see R. v. Milden Hall Magistrates Courts Ex P Forest Heat D. C. -16/05/1997 Times Law Reports."*

The Respondent has formulated a totally different definition on his web page:

> *"The Commissioner may decide not to investigate your complaint if he thinks it is not serious ("frivolous or vexatious" is the term used in the Data Protection Acts). This does not happen very often. If it does, you will be told by this Office. "*

In his letter from October 11th 2013 the Respondent has argued that the law has to be interpreted (different from the above meanings) as:

> *"In a legal context, and for the purposes of Section 10(1)(b)(i) of the DP Acts, the words mean that the Complaint is futile, misconceived, academic and/or not capable of being sustained*".

By using this definition the Respondent is employing a definition that in fact describes complaints that are merely "not justified" and should according to the DPA lead to a formal rejection, which is subject to an appeal at the Circuit Court.

In fact any complaint that is merely "not justified" will practically always fall under the definition "not capable of being sustained". This extremely broad definition makes a narrow exception to the general rule for practically all complaints that the Respondent does not uphold. This comes with the consequence that there is no practical judicial redress for the average complainant.

It will be contended that the decision in *Nowak* clarifies that only complaints which could not possibly achieve the desired outcome could be disposed of as frivolous or vexatious, otherwise such complaints (and in particular the complaint the subject of these proceedings) may only lawfully be disposed of through an investigation by the Respondent.

In addition the Rule of Law calls for a transparent statement by the executive of the circumstances in which it will exercise statutory discretions, particularly where they are broad discretions affecting important rights of individuals - so held the UK Supreme Court in the recent judgment in R (Lumba) v. Secretary of State for the Home Department [2011] UKSC 12,[2012] 1 AC.

If the policy applied by the Respondent is unknown to the Applicant, he cannot make effective representations. The above case will be relied upon in this regard. The Applicant was informed by the Respondent that the interpretation applied to the term "frivolous and vexatious" would be "serious". The Applicant was (reasonably, it is submitted) of the view that there would be no doubt that his complaint was "serious", given that it revealed a possibility, if not probability, that the fundamental right to privacy in respect of approximately one billion

persons had been, and were continuing to be breached. However an entirely different interpretation was applied by the Data Protection Commissioner in arriving at the decision to refuse to investigate as explained in correspondence from the Respondent. In the circumstances the Applicant was entitled to be informed of any relevant policy, or the absence thereof, or any change in policy, prior to a final decision being reached. However it will be submitted that the Applicant was misled as to the policy, or interpretation of "frivolous and vexatious" which would be applied. Had the Applicant been informed of the policy or interpretation actually applied he would have been better equipped to make effective representations.

Ground 5

Ground 5 states:

"The opinion of the Respondent that the complaint was frivolous and vexatious was irrational in the light of the claims made. The Respondent has not assessed the claims made, but based his opinion on matters that are irrelevant to the claims by the Applicant".

The Respondent has in his responses misinterpreted the Applicant's complaint. In his response the Respondent has only explained that

a) Facebook Inc. has self-certified under the Safe Harbour system and

b) there is an exception for law enforcement activities in the Safe Harbour decision.

These two facts were obvious and well known to the Applicant and did not address the complaints made, and were irrelevant to the complaint. The Applicant's complaint was not addressed at all.

Ground 6

Ground 6 states:

"It was ultra vires the power of the Respondent to refuse to consider the Applicant's complaint in circumstances where there was no valid basis to consider the Applicant's complaint as being "frivolous and vexatious"".

The Respondent went beyond his powers in refusing to consider the Applicant's application on its merits. It will be submitted that the Respondent had a duty to investigate the complaint under domestic and EU law (in particular the Data Protection Acts 1988-2003, Directive 95/46/EG, Article 8 CFR and Article 4(3) TFEU) and, in failing to do so, acted ultra vires, thus rendering the impugned decision invalid.

Ground 9

Ground 9 states:

"The decision was based on irrelevant factual considerations. In particular and without prejudice to the generality of the foregoing the question of whether the Applicant's own data was transferred to a third country was of no relevance to the claim made and the refusal to consider the Applicant's complaint".

It is pointed out that a typographical error appears in this Ground and the words "third country" should in fact read "the NSA".

Article 25 of Directive 95/46/EC is regulating that data is transferred to a territory without adequate protection. It is irrelevant if the data is then misused in this territory, just the fact that it was exported out of the EEA is in itself a violation of the data subjects' rights. The claim by the Respondent that there is no proof of any misuse of the Applicant's data after it was transferred to the United States is irrelevant.

Grounds 10 & 8

Ground 10 states:

"The decision to refuse to investigate the Applicant's complaint was arrived in breach of the principle of good administration. No proper reasons were provided for reaching the decision. Numerous arguments put forward by the Applicant in his complaint were not addressed at all.

In particular and without prejudice to the generality of the foregoing no regard was had to the argument of the Applicant in relation to the validity of Decision C2000/520/EC and the scope of its exceptions, "purpose limitation" and "proportionality" as set out in the applicant's complaint. Furthermore had the Applicant's right to good administration been respected and applied then a different and more favourable decision might have been arrived at in respect of the Applicant's Complaint".

Ground 8 states:

"The decision not to investigate the Applicant's complaint was arrived at in breach of the Applicant's fundamental right to be heard. The core aspects of the complaint were not considered at all".

It is submitted that Articles 47 and/or 48 and/or 41(2) of the Charter of Fundamental Rights of the European Union have been breached in arriving at the decision. There was a failure to address the content of the Applicant's representations. The recent Judgment of the CJEU in the Case 277/ 11 will be relied upon and in particular reference will be made to paragraph 88 of that Judgment.

Ground 11

Ground 11 states:

"The refusal to investigate the Applicant's complaint placed an unlawful obstacle in the way of the Applicant's attempt to exercise EU law rights".

Member States have a duty to implement and enforce all EU law (Article 4(3) TEU). In addition Member States have the duty to provide "effective" procedures that do not render it virtually impossible or excessively difficult to exercise rights based on EU law (see e.g. CJEU in C-426/05, p 54). If the Respondent can make it practically impossible or at least very expensive for a EU citizen from another country to exercise his fundamental rights, by pronouncing a complaint "frivolous or vexatious" the EU law's principle of effectiveness is violated.

Ground 12 states:
"The Respondent misinterpreted the Data Protection Acts, and particularly section 10 (1) (a) and 10 (1) (b) thereof, and the legal effect thereof, in arriving at the decision not to investigate".

In relation to this ground the arguments employed under Ground 4 above will be relied upon.

Ground 13
Ground 13 states:
"Insofar as the rights contained in the ECHR constitute general principles of European law and otherwise then the refusal to investigate the Applicant's complaint was in breach of the Applicant's rights under Articles 6 and 8 thereof".

It will be argued, that there is a duty of the member states and all its authorities, lawmakers and courts, to not only not intervene with the fundamental rights of a person, but also defend the fundamental rights of a person against third party violations. In this case Ireland and more specifically the Respondent had a duty under Article 8 ECHR to take all reasonable steps to protect the Applicant against an illegal use of his personal data. Article 13 of the ECHR also enshrines an effective remedy for any such violation. The Applicant further has a right to a fair procedure under Article 6 ECHR which was violated by the Responded.

The Applicant reserves the right to make further submissions prior to or at the hearing of the Application.

Paul O'Shea

THE HIGH COURT
JUDICIAL REVIEW
Record No. 2013/765/JR

BETWEEN:

MAXIMILIAN SCHREMS

APPLICANT

AND

DATA PROTECTION COMMISSIONER

RESPONDENT

SUPPLEMENTAL SUBMISSIONS

Filed on behalf of the applicant on the 22nd day of April 2014 by Ahern Rudden Solicitors, of 5 Clare Street, Dublin 2.

INTRODUCTION

The Applicant intends to rely on the following additional submissions / authorities at the hearing of this application:

1. Decision of the European Court of Justice in the joined Cases C-293/12 and C-594/12 ("Data Retention")

In addition to previous submissions, it is further submitted that the judgment in joined cases C-293/12 and C-594/12 of April 8th 2014 of the ECJ in relation to the interpretation of Article 8 CFR is of relevance. The ECJ has made clear in this judgment that Article 8 CFR does not allow for a blanket collection of personal data for law enforcement, terror prevention and other such purposes. As this is true for the mere collection of meta data, this must consequently also apply to the mass access to content data. In the previously cited judgment C-465/00 the ECJ has made clear that Directive 95/46/EC is to be interpreted with Article 8 ECHR and respectively Article 8 CFR. This also includes the term "adequate protection" in Article 25 of Directive 95/46/EC. Jointly read this means that a transfer of data to a third country that is then accessing content and meta data in bulk cannot be legal under Article 8 CFR. This legal view was equally expressed in the initial complaint of the Applicant.

2. Opinion 04/2014 of the Article 29 Working Party (WP 215)

On April 10th 2014 the Article 29 Working Party (representing the national Data Protection Authorities of all EU Member States) has issued "Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes" which is again – as in previous publications – following the legal view expressed in the initial complaints of the Applicant.

3. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

On April 16th the Committee of Ministers of the Council of Europe has issued a relevant document on the Human Rights for Internet users, stressing that signatory states of the ECHR have a duty to protect the rights of users against private entities and the duty of signatory states to provide an effective remedy. This legal view was equally expressed in the initial complaint of the Applicant.

The Applicant reserves the right to make further submissions prior to or at the hearing of the Application.

Paul O'Shea